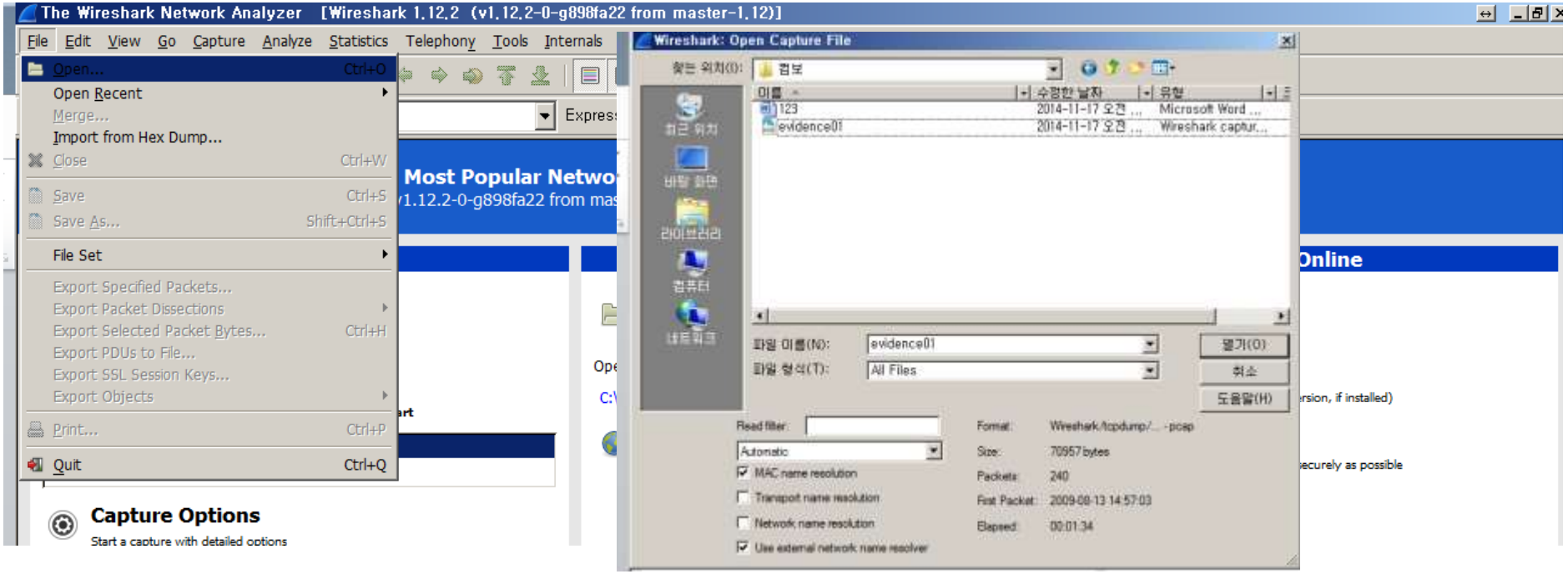
보안실습 8

[네트워크 트래픽에서 파일 추출하기]

준비물: Wireshark, evidence04.pcap, HexaEdit(Winhex)

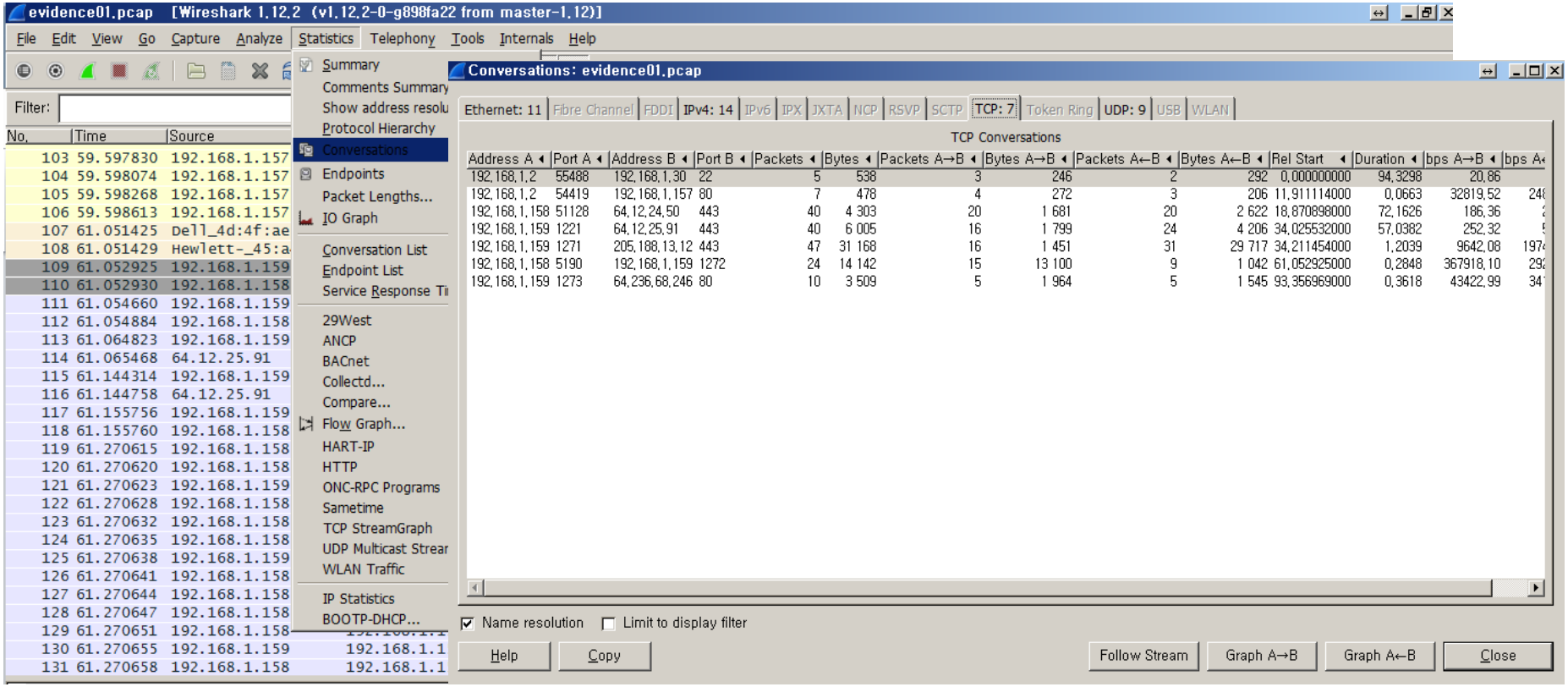
트래픽 캡쳐 파일 열기 (evidence04.pcap)



보안실습 8

[네트워크 트래픽에서 파일 추출하기]

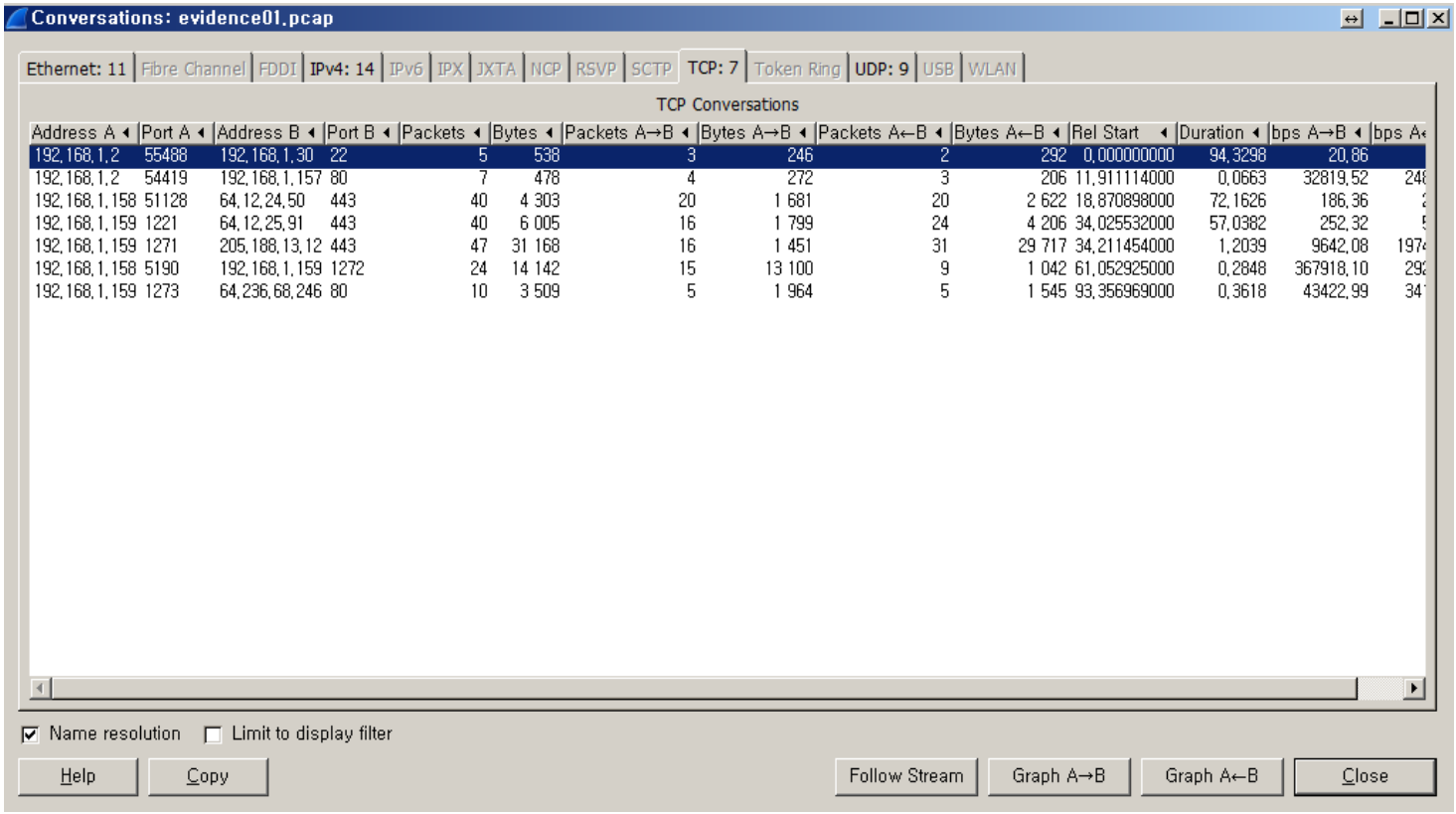
[Conversation] 기능을 통해 호스트간의 트래픽 확인



보안실습 8

[네트워크 트래픽에서 파일 추출하기]

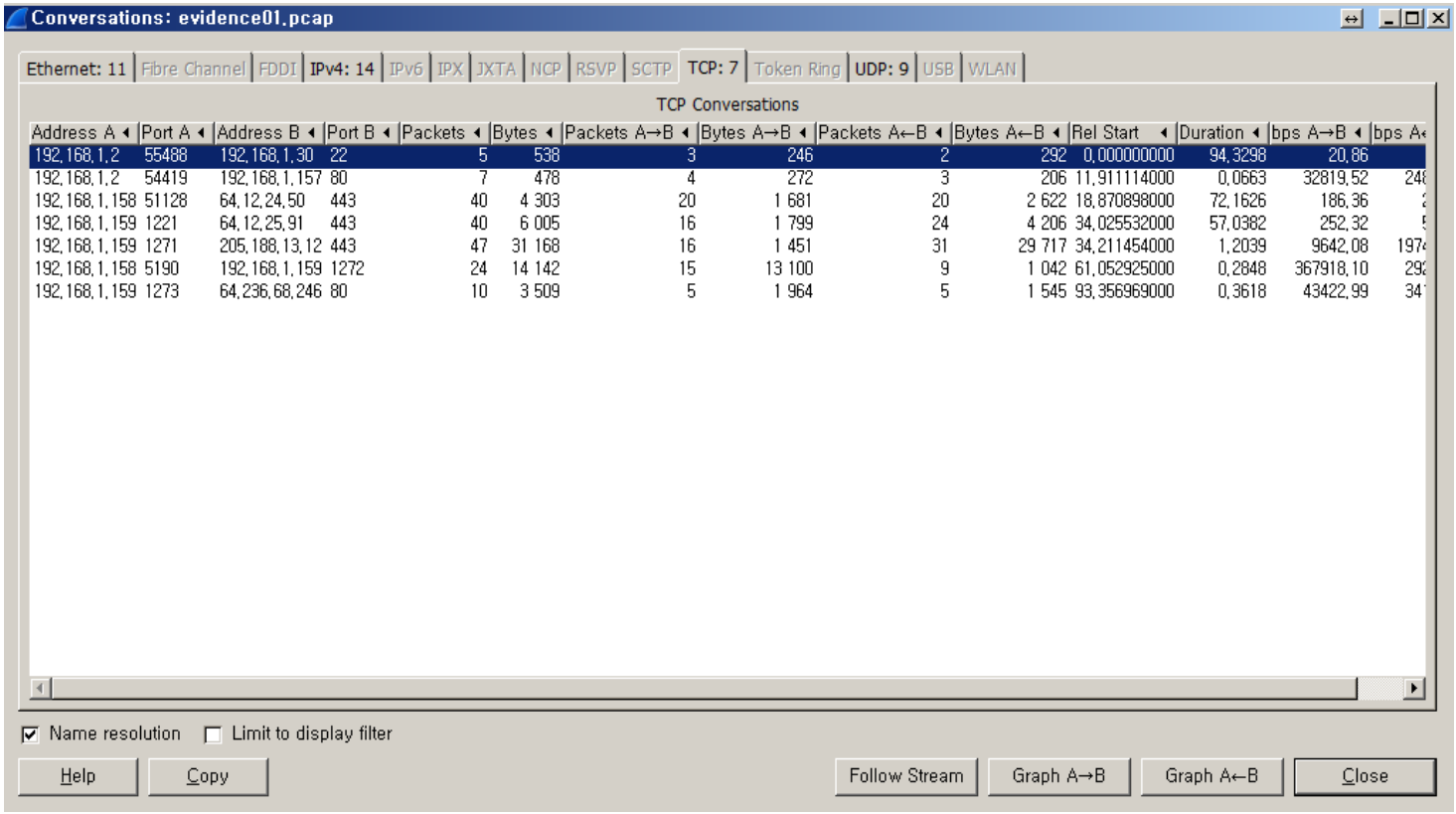
[Conversation] 기능을 통해 호스트간의 트래픽 확인



보안실습 8

[네트워크 트래픽에서 파일 추출하기]

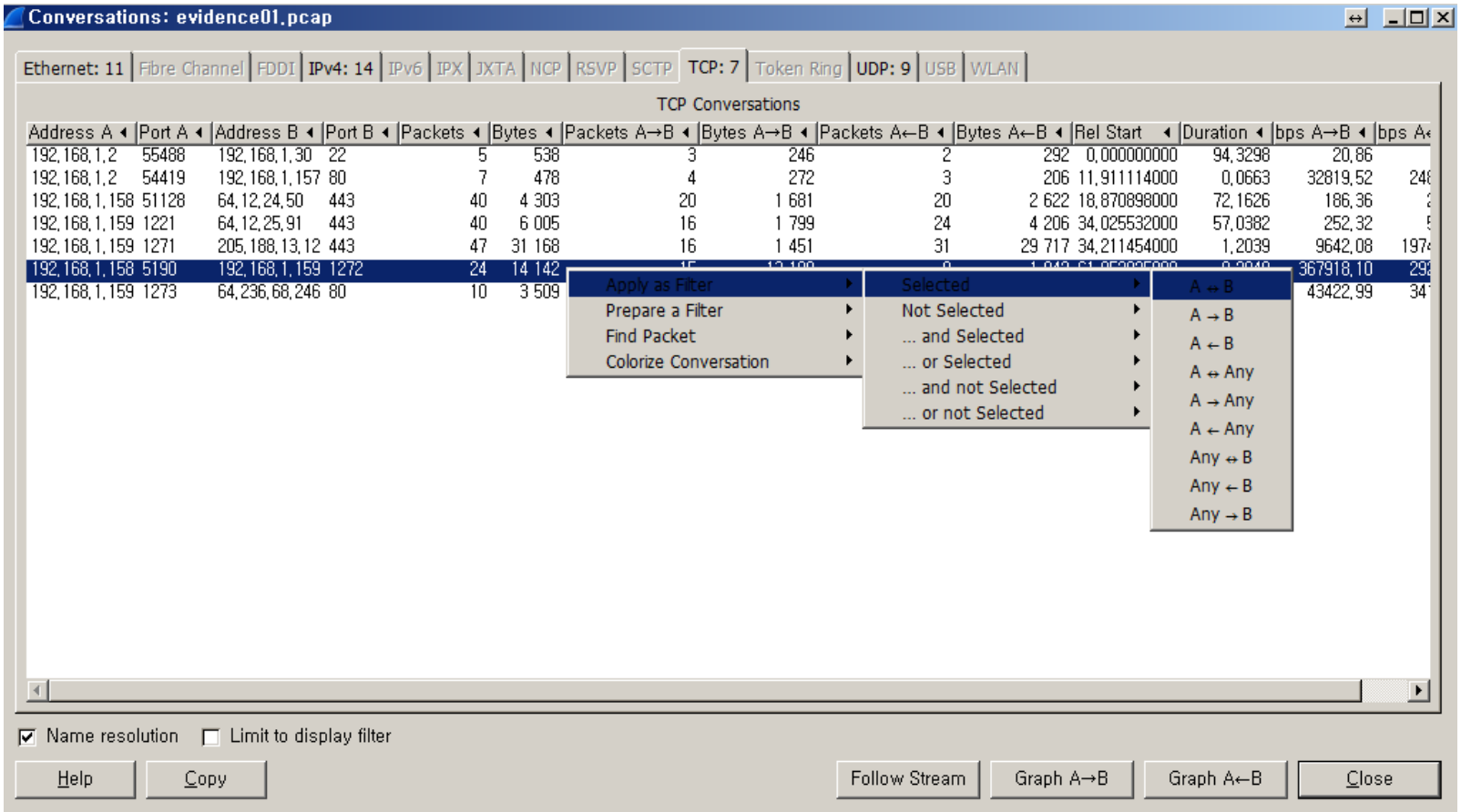
[Conversation] 기능을 통해 호스트간의 트래픽 확인



보안실습 8

[네트워크 트래픽에서 파일 추출하기]

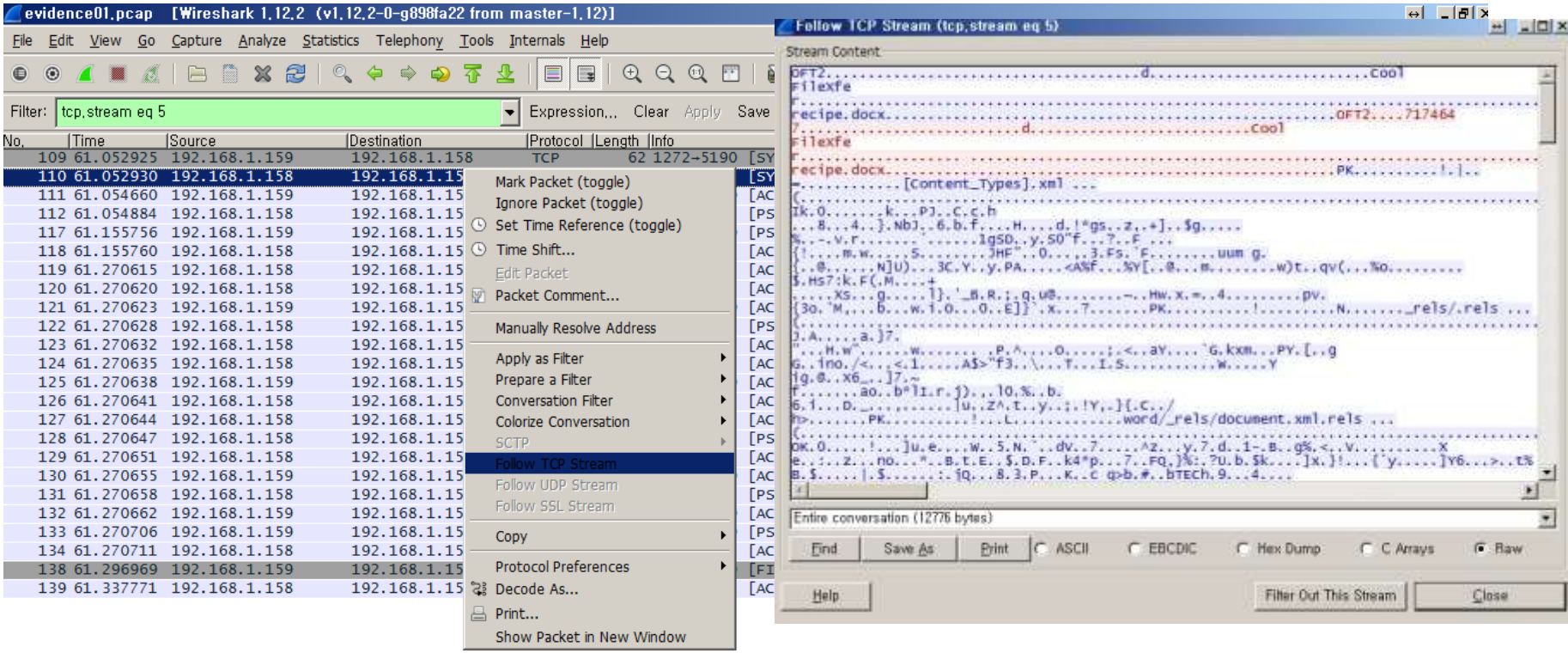
통신 내역 확인



보안실습 8

[네트워크 트래픽에서 파일 추출하기]

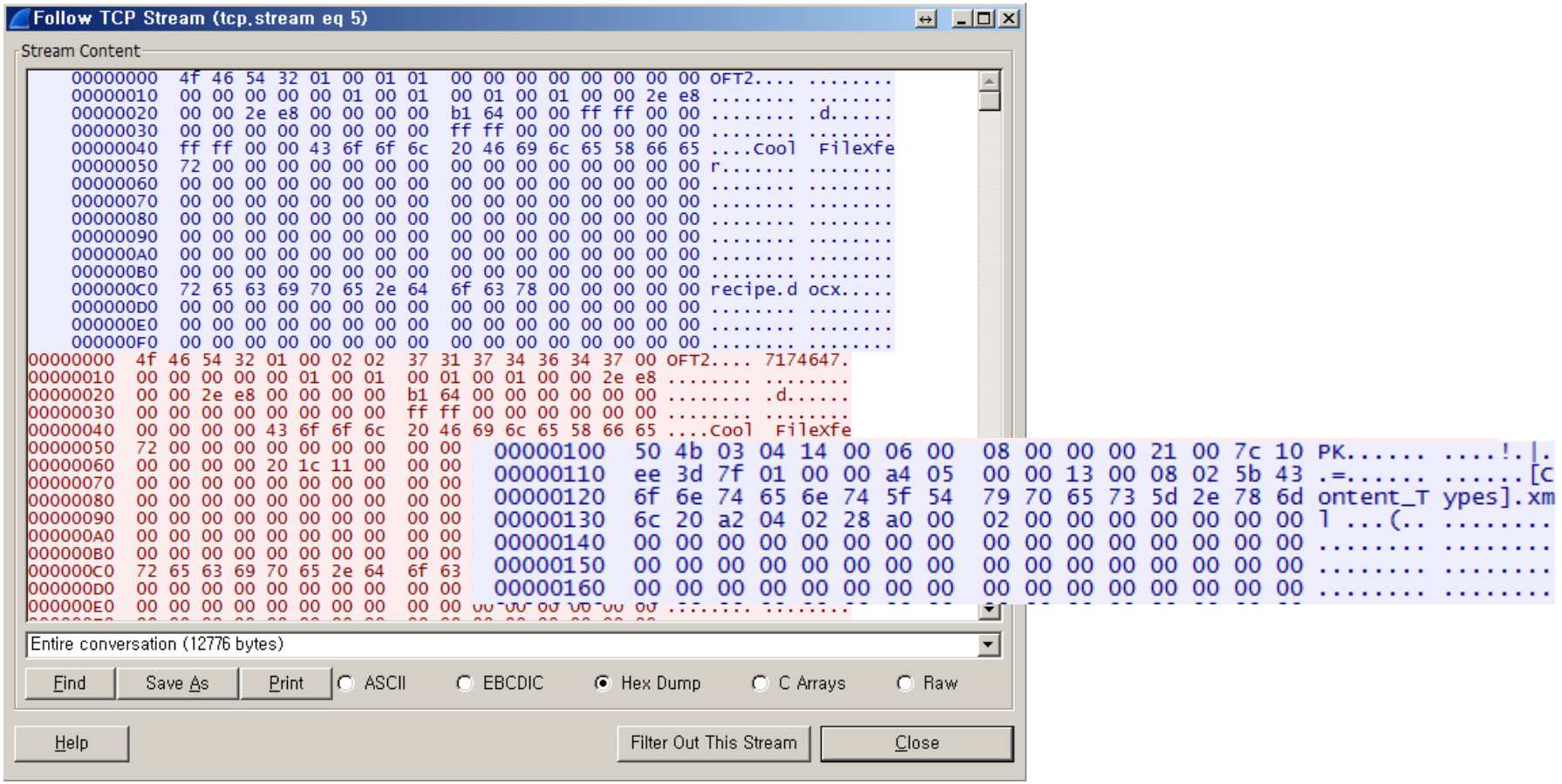
[Follow TCP Stream] 기능을 이용한 트래픽 확인



보안실습 8

[네트워크 트래픽에서 파일 추출하기]

[Hex Dump]로 포맷을 변경 -> PK.. 확인 (매직넘버)



보안실습 8

[네트워크 트래픽에서 파일 추출하기]

[Hex Dump]로 포맷을 변경 -> PK.. 확인 (매직넘버)

```
00000100  50 4b 03 04 14 00 06 00  08 00 00 00 21 00 7c 10 PK...... ....!.|.
00000110  ee 3d 7f 01 00 00 a4 05  00 00 13 00 08 02 5b 43 .=...... ......[C
00000120  6f 6e 74 65 6e 74 5f 54  79 70 65 73 5d 2e 78 6d ontent_T ypes].xm
00000130  6c 20 a2 04 02 28 a0 00  02 00 00 00 00 00 00 00 l ...(.. ........
00000140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
00000160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00 ........ ........
```

검색페이지에서 PK의 16진수 값 뒤에 함께 오는 값을 검색해 보면,
OFFICE 계열의 포멧이라는 것을 확인할 수가 있다.

50 4B 03 04 14 00 06 00
DOCX, PPTX, XLSX

PK.....
Microsoft Office Open XML Format (OOXML) Document
NOTE: There is no subheader for MS OOXML files as there is with DOC, PPT, and XLS files. To better understand the format of these files, rename any OOXML file to have a .ZIP extension and then unZIP the file: look at the resultant file named *[Content_Types].xml* to see the content types. In particular, look for the *<Override PartName=* tag, where you will find *word*, *ppt*, or *xl*, respectively.

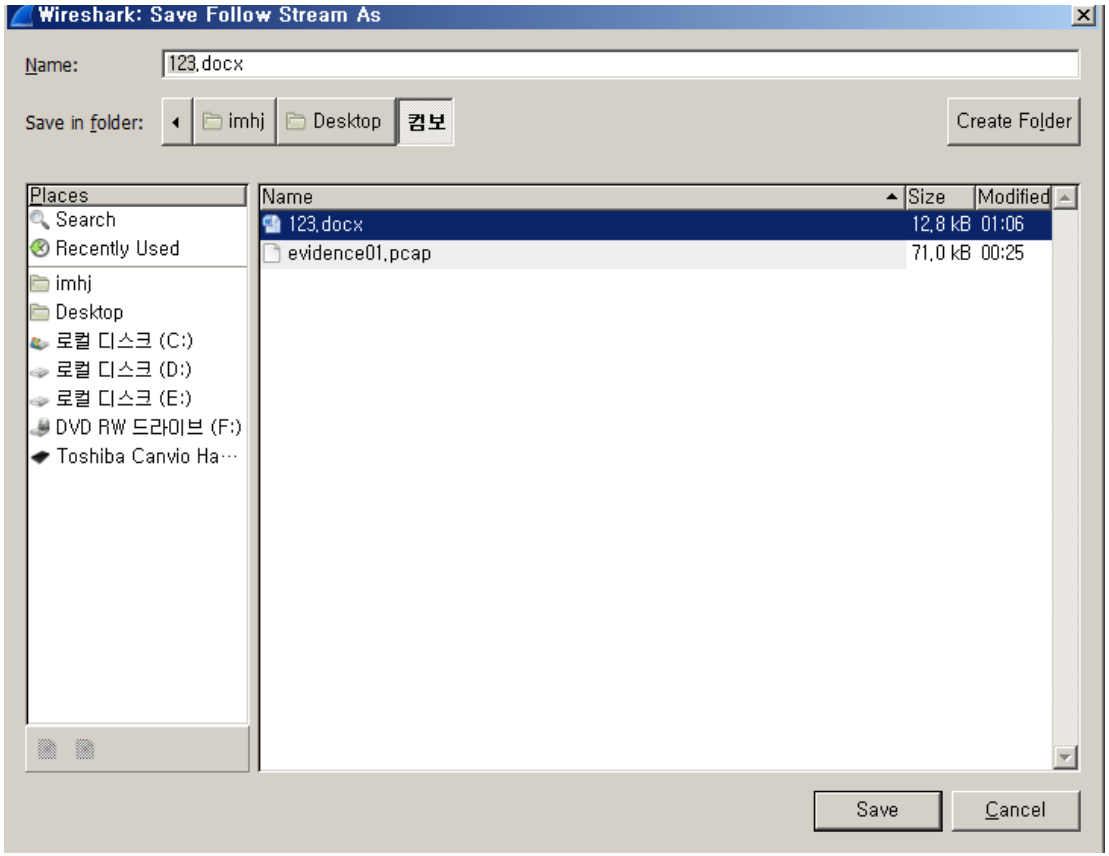
Trailer: Look for 50 4B 05 06 (PK..) followed by 18 additional bytes at the end of the file.

이로써 해당 블록이 OFT2 블록에서 보였던 recipe.docx라고 가정하고 접근해 볼 수 있다.

보안실습 8

[네트워크 트래픽에서 파일 추출하기]

[Hex Dump]로 포맷을 변경 -> PK.. 확인 (매직넘버)



보안실습 8

[네트워크 트래픽에서 파일 추출하기]

Winhex를 통해 필요없는 부분 자르기

Recipe for Disaster:

1 serving

Ingredients:

4 cups sugar

2 cups water

In a medium saucepan, bring the water to a boil. Add sugar. Stir gently over low heat until sugar is fully dissolved. Remove the saucepan from heat. Allow to cool completely. Pour into gas tank. Repeat as necessary.